PRESERVATION AND MANAGEMENT OF DIGITAL LAW RECORDS IN NIGERIA

Justice Chinonso Ujoumunna
Department of Library and Information Science, Abia State University, Uturu, Nigeria
&
Victoria Stobo, PhD
Department of History, Liverpool University Center for Archives Studies,
United Kingdom, England
&
James Lowery, PhD
School of library and Information Studies, Queens College, City University of New York

INTRODUCTION

This chapter discusses preservation and management of digital law records in Nigerian context, in particular reviewing preservation of evidence in digital law records other than law information materials in general. This is to ensure that evidential weight of digital law records are preserved from time of creation to deposal time. In the present -day democracy, the judiciary has been considered a place for justice distribution, crime prevention and rights of the citizens' watch-dog. Therefore, this chapter looks at the Nigerian legal system as a means of solving crimes, peace and conflict resolutions through the admissibility of digital records as digital evidence. This is more so as technology has become the practice and means of communication where peoples' interaction and daily life are resided to survive, hence the need to collect and preserve this activities for future references. The overall objective of this chapter is to discuss the possible professional standards in archival professional viewpoint and digital records management practices hoe to ensure digital law records remain what they purport to document from time of creation, storage to retrieval period when such digital records could be called for to support a fact in any legal proceedings. It also aimed at discussing what constitutes digital records in the legal profession before contemplating whether such digital law records could be preserved with evidential weight for admissibility of digital evidence.

Records: Conceptual Explanation

A record is a specific piece of information produced or received in the initiation, conduct or completion of an institutional or individual activity over time. It comprises sufficient content, context and structure to provide evidence of that activity in a progressive manner for further use. It is not ephemera: that is to say, it contains information that is worthy of preservation and management in the short, medium or long term (Mcleed & Hare, 2006). From the above definition, one can identify concepts which are essential to the definition of records such as content, context, medium and structure. This could be used as carrier of information and proof of one's business activities over time.

Yorke (2000) maintains that for an organization to remain a functioning business entity, it has to create, keep, and mange a wide range of records showing the transactions of the organization within a given period of time. He went further to state that recordkeeping practices within an organization are (in broad terms) a reflection of its particular responses to the environment in which it operates. Expressing his view on the concept of what period of time he states that record is governed by a host of factors and many of these may be outside of the organization. This could be the requirements of admissibility as provided in the provisions of the Evidence Act, (2011) and other laws governing management and admissibility of records in the legal system.

Ujoumunna and Ezenwuzor (2019) see records as "a specific type of documents that can serve as legal evidence, as such, records are often necessary in order to prove compliance, regulation and law". A record is a collection of fields, possibly of different data types, typically in fixed number and sequence. Also, Association of Records Mangers and Administrators International (ARMA) (1992) defines record "as stored information regardless of media or characteristics, created or received by an individual or group which is evidence of its operations and has value requiring its retention for a specific meaningful period of time". In this case, from the definition above, it is

important to state in the content of this discussion that records reviewing under this chapter are not just any kind of document, rather, digital law records which are to be accepted and admissible with enough evidential value, it must have sufficient value to qualify as a record and to be retained as a future evidence of an action or operation especially in courts of law in Nigeria.

Other definition of records by ARMA is stated as “a thing constituting a piece of evidence about the past, especially an account kept in writing or some other permanent form”. The International Standards Organization defines **records** as “information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business”. Whilst useful in stressing the essential evidential quality of a record and of highlighting the vital role played by the record as the output of a transaction, it could be said that this definition of a record fails to adequately describe the properties which define a record (ISO, 2016).

The International Council on Archives (ICA) Committee on Electronic Records defines a **record** as “recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity”. The International Council on Archives goes some way broader to addressing these short-comings by stressing three key properties inherent in all records, that is; that they must possess (ICA, 2005) such as;

- **Content** (ie, information or data)
- **Context** (ie, it must be possible to ascertain how it relates to other records and to the organization which created it)
- **Structure** (ie, there must be an inherent logic to the way in which the information it contains – and the metadata which is likely to define its context – are laid out and which is ultimately interpretable by the human eye).

The result of adhering to these properties should be to create records which contain

the following qualities:

- Authenticity. It should be possible to identify, and preferably prove, the process which created the record and who its authorized creator was
- Completeness. The record should contain all of the content required to act as evidence of the transaction it is documenting. This does not mean that one record must contain Everything to which it relates; simply that it is complete in its own terms
- Reliability. It is important that the content of the record can be relied upon as an accurate representation of the transaction it is documenting
- Fixity. Once declared as a record its content should no longer be altered or changed in any way. It is in this way that its evidential value is preserved (by ensuring that the content of a record remains exactly as it was at creation).

In the words of Parker (1999) records are "documents or other items containing recorded information, which are produced or received as part of a business activity". A document or record can be in any medium and format namely: paper, film, magnetic disks and tapes, optical mediums which can be in any size or type, including microfilm.

Finally, it should be noted that all of the above properties and qualities can apply regardless of the record's format, whether it be a sheet of paper, email, and photograph or database entry. Such precise definitions and their theoretical underpinnings may seem complex and largely irrelevant to practitioners at the 'coal face' within institutions. However, as we shall see throughout the remainder of this strand of the guide they are relevant and do have a very real and practical application. It is largely this definition of what records are that separates them from other types of information or data, and provides them with their added value and, as we shall see, this defines the way in which they must be managed and preserved.

Conceptualizing the meaning of records, Mcleed and Hare (2010) identifies the purpose, value and roles of records as: The purposes of records are namely: 'information (i.e. to ensure that operators are carried out appropriately and to aid

decision-making), for evidence (i.e. as proof that your organization routinely follows consistent practices and for use if the organization is faced with a lawsuit, and as a record of social and historical events). For compliance (i.e. as proof, those regulations have been applied)'. They went further to state the values as in namely: Administrative (i.e. value in relation to the role they play in the everyday operations of the business; example would be records to do with routine correspondences, staff timekeeping, requisitions). Fiscal (i.e. value in relation to financial matters; examples would have administrative value which being processed would include income and expenditure records, which would have administrative value within the context of audit procedures, for the calculation of VAT liability for instance. Legal (i.e. value as proof of compliance with statutory requirement; examples would be deeds and contracts or a Health and Safety certificates. Then, finally, records play evidential and informational or historical roles.

A record's reliability depends on the degree of completeness of its form and on the degree of control exercised over its procedure of creation. The latter includes the control exercised over the author, who must be competent for issuing the special record, that is, must have both the authority and the capacity to do so, and who must be responsible for the recording of the message in the record. A record's authenticity depends on its mode, form, and state of transmission, and on the manner of their preservation and custody. In order to establish the terms of reference and parameters for the development of strategies, procedures, and standards ensuring the reliability and authenticity of electronic records, it is essential to be able to segregate electronic records from other forms of digital information (Duranti, 1991).

Finally based on the above, records could be defined as important daily keeping of activities in either paper or digital format by an individual, private or public, or organizations for future reference purposes which can be used as records of evidence in legal proceedings.

DIGITAL RECORDS: GENERAL OVERVIEW

Digital records are documents in an electronic media. It could be generated in

any computer related devices such as the computer itself or its peripheries. In defining digital record, one may start with machine-readable which is also a digital record; automated record, and or largely obsolete. Put further, Data or information that has been captured and fixed for storage and manipulation in an automated system and that requires the use of the system to render it intelligible by a person can be called a digital record as well.

Digital records' can encompass both analog and digital information formats, although the term principally connotes information stored in digital computer systems. 'Digital records' most often refer to records created in electronic format (born digital) but is sometimes used to describe scans of records in other formats (reborn digital or born analog). Digital records are often analogous to paper records; email to letters, word processing files to reports and other documents. Digital records often have more complex forms, such as databases and geographic information systems.

In Digital Preservation scholars see digital records as not simply the 21st century equivalent of traditional paper records. They have other properties, characteristics and applications. However, both digital and paper records must meet the same legal requirements. In practice, this requires a different approach. Digital records are not tangible objects like a book or a magazine, but a combination of hardware, software and computer files. This combination is necessary to be able to use the documents or examine them. In the context of Testbed, they looked specifically at text documents, databases, email messages and spreadsheets. Multimedia documents, digital video and sound can also be digital records. An important difference compared to paper records is the greater loss of information that can occur even while the records are being used, or afterwards when the records are being maintained. After all, hard discs and computers are replaced regularly and there are few barriers to destroying computer files. A single click on the 'delete' button and a record disappears without leaving a trace (Testbed, 2003).

Going further, Duranti (1998) sees digital records as not always copies of documents because a copy is by definition a reproduction of an original, a draft or another copy (the first copy made is always a reproduction of a document in a different status of transmission); therefore, digital records having a different status of

transmission must be created for copies to exist. It is more appropriate to say that digital records are all made as drafts and received as originals, in consideration of the fact that the records received contain elements automatically added by the system which are not included in the documents sent, and which make them complete and effective at all times as valuable and original.

Again, in an examination of what constitutes digital record, Duranti & MacNeil states the components of digital records just like every traditional record, is comprised of medium (the physical carrier of the message), form (the rules of representation that allow for the communication of the message), persons (the entities acting by means of the record), action (the exercise of will that originates the record as a means of creating, maintaining, changing, or extinguishing situations), context (the juridical-administrative framework in which the action takes place), archival bond (the relationship that links each record to the previous and subsequent one and to all those which participate in the same activity), and content (the message that the record is intended to convey) (Duranti & MacNeil, 1996). However, with digital records, those components are not inextricably joined one to the other, as in traditional records: they, and their parts, exist separately, and can be managed and preserved separately, unless they are consciously tied together for the purpose of ensuring the creation of reliable records and the preservation of authentic records for legal purposes.

An article from InterPARES Authenticity confirms that it is not possible to preserve a digital record. It is always necessary to retrieve from storage the binary digits that make up the record and process them through some software for delivery or presentation. Suderman states that “records in the electronic environment have unique characteristics . . . durability; lifespan; maintenance; ease of editing, copying, erasure, and reformatting (manipulability); ease of manipulation, including the difficulty of tracing manipulation; need for supporting documentation to describe the contents, arrangement, codes, and technical characteristics; need for specialized personnel for the processing and maintenance of the records, introducing a new player in the normal clique of archivist, creator, and user” (Suderman, 2001).

The Electronic Evidence Act, 2011 Section 84 in an attempt to incorporate digital records as admissible records of evidence in the Nigerian Legal System and similar to

the 65B of the Indian Evidence Act, 1872 has in Section these similar contents stated: Admissibility of electronic records.-

(1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:-

(a) The computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer.

(b) During the period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities.

(c) Throughout the material part of the period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and

(d) The information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

From the above contents of the Evidence Acts of Nigeria and Indian with its

similar descriptions, there are two important things to note from the said Acts, namely; (1) the definition of a digital record, (2) the conditions of admissibility in court of law, and perhaps some of the characteristics of an electronic record. One major feature thing to note from the Act, even as accepted by records managers and other legal archivist is those records immanent from constant and normal daily activities and not just what is generated for a purpose.

It is worthy to consider therefore that in managing digital records as admissible records of evidence in courts of law, it must have been that such devices from which the document is presented must have mantled before the incidents occurs. Put simply, computer devices like digital records, CCTVs, audio recording devices, computer in banking institutions used for daily banking transactions are admissible records of evidence and should be used as in original and oral evidence once certified and authenticated. In the other hand, cell phones, and other improvised devices before use should be authenticated as to the electronic signature of such digital records.

DIGITAL EVIDENCE

The clarification of this concept is very important to this chapter. The writer's believe is from the fact that before any analysis can be undertaken of the digital law records and its preservation, it is necessary to understand the need to manage such records which is the application of digital law records in the law of evidence as digital evidence, therefore the real meaning of the term and its underlying nature should be conceptualized. From the reference and reviews of the Evidence Act, 2011, there is no clear-cut or direct definition of the digital evidence. This may be a deliberate and careful act of the lawmakers to avoid some unforeseen circumstance of given a precise definition or perhaps future treatment of the definition to what technology may explore. The term electronic as a generic word which encompasses all forms of data, whether produced by an analog device, or digital form (Mason, 2017). He went further to add that digital evidence is:

> Data (comprising the output of analogue devices or data in digital format) that is created, manipulated, store or communicated by any devices, computer or computer systems or transmitted over a communication system that is relevant

to the process of adjudication.

Ten years after as noted by Ajileye (2004) he observes that in the recent work modified by Schafer & Mason, Electronic evidence: Disclosure, Discovery and Admissibility, revised edition, (2019) the former definition by Mason was modified by removing the words, “relevant and adjudication” and replacing same with the words, “that has the potentials to make the factual account of either party more probable or less probable that it would be without evidence. The new definition according to him became:

> Data (comprising the output of analogue devices or data in digital format) that is created, manipulated, store or communicated by any devices, computer or computer systems or transmitted over a communication system that is that has the potentials to make the factual account of either party more probable or less probable that it would be without evidence.

This in one aspect has proven the fact we raised earlier that may have made the lawmakers to avoid a simple definition in the Evidence Act, 2011. The other hand, as emphasized by Ajileye (2018:75) he notes three key points in the definition of Schafer and Mason (2017:76), stating that the recent definition consists of three elements. They are: first, all forms of data created, manipulated or stored in a computer. Second, it encompasses the various forms of devices by which data can be stored or transmitted, including analog devices that produce output. Third, the definition according to him attempts to take care of the meaning of the word, “evidence” as “information that has the potentials to make the factual account of either party more probable or less probable that it would be without evidence.

Considering the above reviews, digital evidence can be any technological produced record that is admissible in any legal gathering that can cause decisions from the facts proven by the said digital record. It is important to note that such records may be found in such technologies like ATM transaction analyses, CCTV Database, digital audio recorders and cameras, computer memory, satellites, Electronic mails, Facebook, WhatsApp, Twitter, Instagram, Yahoo-messenger, and other social media platforms.

Casey (2014) sees digital evidence or electronic evidence as

“any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required”.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programmes, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System (GPS) tracks, logs from a hotel’s electronic door locks, and digital video or audio files (Various, 2009). Once such contains probative value which could be tendered in court or deliberated generated as reference to activities between two parties, such a digital record is referred to as digital law records.

PRESERVATION AND MANAGEMENT OF DIGITAL LAW RECORDS

Digital records management may be seen as the process of collecting, arranging, classifying and cataloguing, processing and storing as well as disseminating digital records for easy use and retrievals. Managing digital records is also a complex task because it comprises of the entire life-cycle of the record from the creation, collection, classification and analysis, organization and interpretation, storage and retrievals and providing ongoing access to the said records. In managing digital law records, it is important to bear in mind that these records vary in nature; their timely disposal must be arranged for the fixed life, and long-term preservation for those records of historical value. It has become a global view that digital records should be managed even though some countries are yet having challenges from the early stage as technology evolves from time to time.

Law records management, perhaps, digital records concerns multiple roles in that; it covers the organizational, technical and legal issues, and which must be considered in managing records from time to time. McDonald (2005) states that in terms of recordkeeping laws and policies, for instance, some progress have been made

over the past ten years in establishing accountability frameworks for the management of information including information in records. He went on to state that the effective management of digital law records is not just a technology issue but requires an infrastructure of laws and policies, standards and practices, systems and technologies, and leadership capable of continually aligning the infrastructure in support of the business of an organization. It is these lacks of laws, policies and organized systems that many countries like Nigeria are facing in the legal system as a challenge of admissible records in digital format with contemporaneous issues such as evidential weight.

Digital records management is very systematic and goes in a strict consistent control of all records throughout their lifecycle. This means that records need to be managed in a well-planned and methodical design instead of accidental management or request on use approach. In managing digital law records, technology ought to be considered in that records become effective, efficient and consistent part of business activities by evaluating the types of software systems for managing digital law records, procedures for the management of digital law records over time and analysis of approaches to integrating digital law records management in our day to day life since we now live in an electronic environment or digital economy.

ADMISSIBILITY OF DIGITAL RECORDS AS DIGITAL EVIDENCE

Legal admissibility refers to whether a court of law would accept digital file as a valid piece of evidence in case of judging over a dispute. Even though records can be admissible (i.e. accepted as evidence) the opposing party and their legal counsel may call the evidential weight into question if there are any doubts as to the record's veracity or integrity (Ajileye, 2018:334). Digital files must be accurate, i.e. unaltered representations of the information; Digital files must be authentic, i.e. what it purports to be; Digital files must not have been tampered with; Digital files must be stored in a system that is secure throughout the file's lifetime. If you can't demonstrate the above, then the file's evidential weight can be severely called into question in case of a fact under dispute. There are no hard and fast rules to determine whether a digital record is

100% legally admissible, and it remains to say that there are many ways that paper files are commonly manipulated, forged, called into question etc. but it is of course questionable.

SUMMARY

For records to be preserved and managed, the records managers must ensure that the records are created and preserved over time without any intention to support or conceal a fact in favour of evidence. The chapter has been able to discuss the meaning, nature and scope of law records, its preservation and management issues which all points to preserving the evidential qualities of such records from creation to disposal periods. A review of what constitutes law records was also discussed. Admissibility of digital evidence and concept of digital evidence were also discussed.

REFERENCES

Ajileye (2004). Electronic Evidence. In Schafer & Mason, Electronic evidence: Disclosure, Discovery and Admissibility, revised edition, (2019)

Ajileye, A. O. (2018). *Electronic evidence.* Nigerian: Nigerian Jurist Publications Series.

Amagno (2017). Salvatore Coppola-Finegan in his Blog post on Amango website, 2017

ARMA. (1992). Records management roundtable steering committe . In *Electronic records management and archives symposium: A Quarter Century Perspective*, by H Perritt. HeinOline.

Casey, E. (2014). *Digital evidence and computer crime (1st ed.).* London: Academic Press.

Duranti, L.T. (1996). Eastwood, and H MacNeil. *Preservation of the integrity of electronic records.* London: Springer

Duranti, Luciana, T Eastwood, and H MacNeil. (1991). *Preservation of the integrity of electronic records.* london: Springer

Duranti, Luciana. (2001). Concepts, principles, and methods for the management of electronic records. *The Information Society* 17(4): 271-279.

ICA. (2005). International Council of Archives . *Official website of ICA.* https://www.ica.org/en/sites/default/files/ICA_Study-16-Electronic records_EN.pdf (accessed 03 13, 2020).

International Council on Archives (2005). Electronic records: a workbook for Archivists. Committee on current Records in an Electronic Environment. ICA study 16. This workbook is retrieved from https://www.jisc.ac.uk/guides/records-

management/what-is-a-record.

Mason, S. (2017). Sources of digital evidence. In *Electronic evidence: Disclosure, Discovery and admissibility*, by S Mason, 66-89. London: Butterworth

McDonald, S. A. (2005). Authenticating digital evidence from the cloud. *Army Lawyer*, (2005): 40-50.

McLeed, J. & Hare, C (2006). *Managing electronic records,* London: Facet Publishers.

McLeed, J., and C. Hare. (2010). Managing electronic records. In *Electronic records Management*, by J McLeed and C Hare, 456-566. London: Facet Publishers

Parker, E. (199). *Managing your organization's records.* London: Library Association Publishing.

Sara, J. P. (2003). Legal admissibility of electronic records as evidence and implications for records management. *American Archivist* (58): 54-64.

Suderman, C.C.(2011). *Introduction to law of evidence in Nigeria with evidence act 2011.* Nigeria: Mounterest University Press.

Ujoumunna, J. C, & Ezenwuzor, N. L. (2019). Records, retention, retrieval and transfer. In *Records and information management: a fundamental approach*, by J. C. Ujoumunna and O Ugocha, 88-92. Nigeria: Justman Publishers.

Various, C.O. (2009). Admissibility of electroinc and computer-genterated evidence in Nigeria: issuess and responses; *International Journal of Advanced Scientific Research* 2(1): 2559-0094.

Yorke, M., & Knight, P. (2006). *Embedding employability into the curriculum.* New York: Higer Education Academy.